

[19] 中华人民共和国国家知识产权局



# [12] 发明专利申请公布说明书

[21] 申请号 200580023727.0

[51] Int. Cl.

H04L 9/08 (2006.01)

H04L 9/32 (2006.01)

[43] 公开日 2007 年 6 月 20 日

[11] 公开号 CN 1985466A

[22] 申请日 2005.7.8

[21] 申请号 200580023727.0

[30] 优先权

[32] 2004.7.14 [33] US [31] 10/892,280

[86] 国际申请 PCT/US2005/024253 2005.7.8

[87] 国际公布 WO2006/019614 英 2006.2.23

[85] 进入国家阶段日期 2007.1.15

[71] 申请人 英特尔公司

地址 美国加利福尼亚州

[72] 发明人 J·萨顿二世 C·霍尔

E·布瑞克尔 D·格劳罗克

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 顾嘉运

权利要求书 5 页 说明书 13 页 附图 11 页

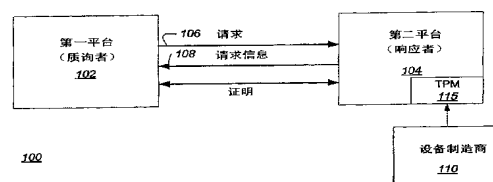
## [54] 发明名称

使用分发 CD 按签署组向设备传递直接证据私钥的方法

## [57] 摘要

现场按经签署的密钥组向客户机计算机系统中安装的设备传递直接证明私钥可用安全的方式来完成，而不需要设备中的大量非易失性存储。生成唯一伪随机值，并将其连同组序号一起在制造时储存在设备中。该伪随机值用于生成用于加密一数据结构的对称密钥，该数据结构持有与该设备相关联的直接证明私钥和私钥摘要。所得的经加密的数据结构被储存在可移动存储介质（诸如 CD 或 DVD）上的经签署的密钥组（例如，经签署的组记录）中，并被分发到计算机系统的所有者。当在客户机计算机系统上初始化设备时，系统核查系统中是否存在本地化的经加密的数据结构。如果没有，则系统从可移动存储介质中获得该相关联的经加密的数据结构的经签署的组记录，并验证该经签署的组记录。当组

记录有效时，设备使用从其所储存的伪随机值重新生成的对称密钥来解密该经加密的数据结构来获得直接证明私钥。如果私钥有效，则它可用于客户机计算机系统设备的后续认证处理。



1. 一种方法，包括：

生成与设备相关联的经加密的数据结构，所述经加密的数据结构包括私钥和私钥摘要；

基于伪随机生成的值为所述经加密的数据结构生成一标识符；

将所述标识符和所述经加密的数据结构储存在可移动存储介质上的经签署的组记录中；以及

将所述伪随机值和对应于所述经签署的组记录的组序号储存在所述设备内的非易失性存储中。

2. 如权利要求 1 所述的方法，其特征在于，还包括分发所述可移动存储介质和所述设备。

3. 如权利要求 1 所述的方法，其特征在于，还包括为一类设备生成直接证明族密钥对。

4. 如权利要求 1 所述的方法，其特征在于，还包括生成用于签署和验证所述组记录的密钥对。

5. 如权利要求 4 所述的方法，其特征在于，还包括将所述组记录的密钥对的公钥的散列储存在所述设备的非易失性存储中。

6. 如权利要求 1 所述的方法，其特征在于，还包括为所述经签署的组记录选择组大小。

7. 如权利要求 3 所述的方法，其特征在于，所述私钥包括与所述直接证明族密钥对的公钥相关联的直接证明私钥，并且所述方法还包括对所述直接证明私钥进行散列运算以生成所述私钥摘要。

8. 如权利要求 1 所述的方法，其特征在于，还包括基于所述设备的伪随机值生成对称密钥。

9. 如权利要求 8 所述的方法，其特征在于，生成所述标识符包括使用所述对称密钥来加密数据值。

10. 如权利要求 8 所述的方法，其特征在于，还包括使用所述对称密钥来加密所述数据结构。

11. 如权利要求 1 所述的方法，其特征在于，所述经加密的数据结构还包括

随机初始化向量。

12. 如权利要求 1 所述的方法, 其特征在于, 所述可移动存储介质包括 CD 和数字多功能盘 (DVD) 中的至少一个。

13. 如权利要求 1 所述的方法, 其特征在于, 所述设备的伪随机值是唯一的。

14. 一种制品, 包括: 具有多个机器可读指令的第一存储介质, 其中当所述指令由处理器执行时, 所述指令能够通过以下步骤按经签署的组将私钥传递到设备:

生成与设备相关联的经加密的数据结构, 所述经加密的数据结构包括私钥和私钥摘要;

基于伪随机生成的值为所述经加密的数据结构生成一标识符;

将所述标识符和所述经加密的数据结构储存在可移动存储介质上的经签署的组记录中; 以及

使得将所述伪随机值和对应于所述经签署的组记录的组序号储存到所述设备内的非易失性存储中。

15. 如权利要求 14 所述的制品, 其特征在于, 还包括用于生成用于签署和验证所述组记录的密钥对的指令。

16. 如权利要求 15 所述的制品, 其特征在于, 还包括用于将所述组记录密钥对的公钥的散列储存在所述设备的非易失性存储中的指令。

17. 如权利要求 14 所述的制品, 其特征在于, 还包括用于为所述经签署的组记录选择组大小的指令。

18. 如权利要求 14 所述的制品, 其特征在于, 还包括用于为一类设备生成直接证明族密钥对的指令。

19. 如权利要求 14 所述的制品, 其特征在于, 所述私钥包括与所述直接证明族密钥对的公钥相关联的直接证明私钥, 并且还包括用于对所述直接证明私钥进行散列运算以生成所述私钥摘要的指令。

20. 如权利要求 14 所述的制品, 其特征在于, 还包括用于基于所述设备的伪随机值生成对称密钥的指令。

21. 如权利要求 20 所述的制品, 其特征在于, 所述用于生成标识符的指令包括用于使用所述对称密钥来加密数据值的指令。

22. 如权利要求 20 所述的制品, 其特征在于, 还包括用于使用所述对称密钥来加密所述数据结构的指令。

23. 如权利要求 14 所述的制品, 其特征在于, 所述经加密的数据结构还包括随机初始化向量。

24. 如权利要求 14 所述的制品, 其特征在于, 所述设备的伪随机值是唯一的。

25. 一种方法, 包括:

确定与安装在计算机系统上的设备相关联的经加密的数据结构是否储存在所述计算机系统上的存储器中, 所述经加密的数据结构包括私钥和私钥摘要; 以及

如果未储存所述经加密的数据结构, 则按经签署的组记录从可由所述计算机系统访问的可移动存储介质中获取与所述设备相关联的经加密的数据结构, 所述可移动存储介质储存经签署的组记录的数据库。

26. 如权利要求 25 所述的方法, 其特征在于, 所述可移动存储介质包括由所述设备的制造商生产的 CD 和数字多功能盘 (DVD) 中的至少一个。

27. 如权利要求 25 所述的方法, 其特征在于, 获取所述经加密的数据结构包括向所述设备发出获取密钥命令以启动私钥获取过程。

28. 如权利要求 25 所述的方法, 其特征在于, 所述私钥包括与用于一类设备的直接证明族密钥对的公钥相关联的直接证明私钥。

29. 如权利要求 27 所述的方法, 其特征在于, 所述私钥获取过程包括基于储存在所述设备中的唯一伪随机值来生成对称密钥。

30. 如权利要求 29 所述的方法, 其特征在于, 所述私钥获取过程包括基于所述伪随机值为所述经加密的数据结构生成一设备标识符。

31. 如权利要求 27 所述的方法, 其特征在于, 所述私钥获取过程包括从所述可移动存储介质中获取对应于所述设备的组序号的经签署的组记录。

32. 如权利要求 30 所述的方法, 其特征在于, 还包括对所述经签署的组记录进行语法分析以获得对应于所述设备标识符的组序号、组公钥和经加密的数据结构。

33. 如权利要求 31 所述的方法, 其特征在于, 还包括验证所述经签署的组记录。

34. 如权利要求 32 所述的方法, 其特征在于, 所述私钥获取过程还包括使用所述对称密钥来解密从所述可移动存储介质接收到的经加密的数据结构, 以获得所述私钥和所述私钥摘要。

35. 如权利要求 34 所述的方法, 其特征在于, 所述私钥获取过程还包括对所述私钥进行散列运算以生成新的私钥摘要, 将来自所述经解密的数据结构的私钥摘

要与所述新的私钥摘要进行比较,以及当所述摘要匹配时接受所述私钥作为所述设备的有效私钥。

36. 一种制品, 包括: 具有多个机器可读指令的第一存储介质, 其中当所述指令由处理器执行时, 所述指令能够通过以下步骤从用于安装在计算机系统上的设备的经签署的组记录中获得私钥:

确定与安装在计算机系统上的设备相关联的经加密的数据结构是否被储存在所述计算机系统上的存储器中(904), 所述经加密的数据结构包括私钥和私钥摘要; 以及

如果未储存所述经加密的数据结构, 则按经加密的组记录从可由所述计算机系统访问的可移动存储介质获得与所述设备相关联的经加密的数据结构, 所述可移动存储介质储存经签署的组记录的数据库。

37. 如权利要求 36 所述的制品, 其特征在于, 用于获得所述经加密的数据结构的指令包括用于向所述设备发出获取密钥命令以启动私钥获取过程的指令。

38. 如权利要求 36 所述的制品, 其特征在于, 所述私钥包括与用于一类设备的直接证明族密钥对的公钥相关联的直接证明私钥。

39. 如权利要求 37 所述的制品, 其特征在于, 所述私钥获取过程包括基于储存在所述设备中的唯一伪随机值生成对称密钥。

40. 如权利要求 37 所述的制品, 其特征在于, 所述私钥获取过程包括基于所述伪随机值为所述经加密的数据结构生成一设备标识符。

41. 如权利要求 37 所述的制品, 其特征在于, 所述私钥获取过程包括从所述可移动存储介质中获得对应于所述设备的组序号的经签署的组记录。

42. 如权利要求 40 所述的制品, 其特征在于, 还包括对所述经签署的组记录进行语法分析以获得对应于所述设备标识符的组序号、组公钥和经加密的数据结构。

43. 如权利要求 41 所述的制品, 其特征在于, 还包括验证所述经签署的组记录。

44. 如权利要求 42 所述的制品, 其特征在于, 所述私钥获取过程还包括使用所述对称密钥来解密从所述可移动存储介质接收到的经加密的数据结构以获得所述私钥和所述私钥摘要。

45. 如权利要求 44 所述的方法, 其特征在于, 所述私钥获取过程还包括对所述私钥进行散列运算以生成新的私钥摘要, 将来自所述经解密的数据结构的私钥摘

---

要与所述新的私钥摘要进行比较,以及当所述摘要匹配时接受所述私钥作为对所述设备的有效私钥。

## 使用分发 CD 按签署组向设备传递直接证据私钥的方法

### 背景

#### 1. 领域

本发明一般涉及计算机安全，尤其涉及向处理系统中的设备安全地传递密码密钥。

#### 2. 描述

支持内容保护和/或计算机安全特征的某些处理系统体系结构要求特别保护或“可信的”软件模块能够创建与处理系统中特别保护或“可信的”硬件设备（诸如，例如图形控制卡）的经认证的加密通信会话。一种用于标识设备并同时建立加密通信会话的常用方法是使用单侧经认证的 Diffie-Helman（DH）密钥交换过程。在这一过程中，向设备分配一唯一的公有/私有 Rivest, Shamir and Adelman（RSA）算法密钥对或唯一的 Elliptic Curve Cryptography（椭圆曲线密码，ECC）密钥对。然而，由于该认证过程使用 RSA 或 ECC 密钥，因此设备具有唯一且可证明的身份，这可能会引发私密性问题。在最坏情况下，这些问题会导致缺少原始设备制造商（OEM）对构建提供这种安全性的可信设备的支持。

### 附图简述

阅读以下本发明的详细描述，可以清楚本发明的特征和优点，其中：

图 1 示出了以用根据本发明的一个实施例操作的可信平台模块（TPM）实现的平台为特征的系统；

图 2 示出了包括图 1 的 TPM 的平台的第一实施例；

图 3 示出了包括图 1 的 TPM 的平台第二实施例；

图 4 示出了用图 2 的 TPM 实现的计算机系统的一个示例性实施例；

图 5 是根据本发明的一个实施例用于按签署组来分发直接证明密钥的系统的图示；

图 6 是示出根据本发明的一个实施例的按签署组来分发直接证明密钥的方法

的步骤的流程图；

图 7 和 8 是示出根据本发明的一个实施例的设备制造设置处理的流程图；

图 9 是示出根据本发明的一个实施例的设备制造生产处理的流程图；

图 10 和 11 是根据本发明的一个实施例的客户机计算机系统设置处理的流程图；以及

图 12 是根据本发明的一个实施例的客户机计算机系统处理的流程图。

### 详细描述

使用基于直接证明的 Diffie-Helman 密钥交换协议来允许受保护/可信设备认证它们自己并建立与可信软件模块的加密通信会话避免了在处理系统中创建任何唯一身份信息，并由此避免引入私密性问题。然而，在生产线上的设备中直接嵌入直接证明私钥要求设备上有比其它方法更多的受保护非易失性存储，从而增加了设备成本。本发明的一个实施例是一种允许在分发光盘只读存储器(CD-ROM 或 CD)上以安全的方式按签署组来传递直接证明私钥(例如，用于签署)并随后由设备本身安装在设备中的方法。在一个实施例中，支持这一能力所需的设备存储可以从大约 300 到 700 字节减少到大约 20-25 字节。实现对设备的基于直接证明的 Diffie-Helman 密钥交换所需的非易失性存储的量的减少可导致对这一技术的更广泛采用。

本发明的说明书中对“一个实施例”或“一实施例”的引用指的是结合该实施例描述的特定特征、结构或特性包括在本发明的至少一个实施例中。由此，遍及说明书各处出现的短语“在一个实施例中”不必都指同一实施例。

在以下描述中，使用某些特定术语来描述本发明的一个或多个实施例的某些特定特征。例如，“平台”被定义为适用于发送和接收信息的任何类型的通信设备。各种平台的示例包括但不限于或不约束于计算机系统、个人数字助理、蜂窝电话、机顶盒、传真机、打印机、调制解调器、路由器等。“通信链路”被宽泛地定义为适用于平台的一种或多种信息承载介质。各种类型的通信链路的示例包括但不限于或不约束于电线、光纤、电缆、总线轨迹或无线信令技术。

“质询者”指的是请求对另一实体的真实性或授权进行某种验证的任何实体(例如，个人、平台、系统、软件和/或设备)。通常，这是在公开或提供所请求的信息之前执行的。“响应者”指的是被请求提供关于其授权、有效性和/或身份的某种证明的任何实体。“设备制造商”可与“证明制造商”互换使用，指的是制



造或配置平台或设备的任何实体。

如此处所使用的，向质询者“证明”或使其“确信”响应者拥有某一密码信息（例如，数字签名、诸如密钥等秘密等）或具有关于该信息的信息意味着基于向质询者公开的信息和证明，响应者非常有可能具有该密码信息。在不向质询者“揭示”或“公开”该密码信息的情况下向质询者证明这一点意味着基于向质询者公开的信息，质询者要确定该密码信息在计算上是不可行的。

这一证明在下文中称为直接证明。术语“直接证明”指的是零知识证明，因为这些类型的证明通常是本领域中已知的。特别地，如此处所引用的特定直接证明协议是2002年11月27日提交的名为“System and Method for Establishing Trust Without Revealing Identity”（用于在不揭示身份的情况下建立信任的系统和方法）、转让给本申请的所有者的共同待批的专利申请第10/306,336的主题。直接证明定义了发布者确定如能共享由发布者定义的公共特性的许多成员的族的协议。发布者生成将该族表示为一个整体的族公钥和私钥对（Fpub 和 Fpri）。使用 Fpri，发布者还可为族中的每一个别成员生成唯一的直接证明私有签署密钥（DPpri）。用个别的 DPpri 签署的任何消息可使用族公钥 Fpub 来验证。然而，这一验证仅标识签署者是该族的成员；并不揭露关于该个别成员的唯一标识信息。在一个实施例中，发布者可以是设备制造商或代理。即，发布者可以是具有基于共享特性定义设备族、生成族公钥/私钥对、以及创建 DP 私钥并将其注入到设备中的能力的实体。发布者还可为族公钥生成标识公钥来源以及设备族的特性的证书。

现在参考图1，示出了以用根据本发明的一个实施例操作的可信硬件设备（称为“可信平台模块”或“TPM”）实现的平台为特征的系统的实施例。第一平台102（质询者）发送请求106，第二平台104（响应者）提供关于其本身的信息。响应于请求106，第二平台104提供所请求的信息108。

另外，为提升安全性，第一平台102可能需要验证来自自由选择的一个设备制造商或选择的一组设备制造商（以下称为“设备制造商110”）制造的设备的所请求的信息108。例如，对于本发明的一个实施例，第一平台102质询第二平台104以示出它具有由设备制造商110生成的密码信息（例如，签名）。质询可以被结合在请求106中（如所示出的）或是单独的传输。第二平台104通过以回复的形式提供信息来回复该质询，以使第一平台102确信第二平台104具有由设备制造商110生成的密码信息，而不揭示该密码信息。回复可以是所请求的信息108的一部分（如所示出的），或是单独的传输。

在本发明的一个实施例中，第二平台 104 包括可信平台模块 (TPM) 115。TPM 115 是由设备制造商 110 制造的密码设备。在本发明的一个实施例中，TPM 115 包括具有密封在封装内的少量片上存储器的处理器。TPM 115 被配置成向第一平台 102 提供使其能够确定回复是从有效 TPM 发送的信息。所使用的信息是不会使 TPM 或第二平台的身份可能得到确定的内容。

图 2 示出了具有 TPM 115 的第二平台 104 的第一实施例。对于本发明的该实施例，第二平台 104 包括耦合到 TPM 115 的处理器 202。一般而言，处理器 202 是处理信息的设备。例如，在本发明的一个实施例中，处理器 202 可以被实现为微处理器、数字信号处理器、微控制器或甚至是状态机。或者，在本发明的另一实施例中，处理器 202 可被实现为可编程或硬编码的逻辑，诸如现场可编程门阵列 (FPGA)、晶体管-晶体管逻辑 (TTL) 逻辑、或甚至是专用集成电路 (ASIC)。

此处，第二平台 104 还包括存储单元 206，以允许储存诸如以下的一个或多个等密码信息：密钥、散列值、签名、证书等。“X”的散列值可被表示为“Hash(X)”。可以设想了这一信息可被储存在 TPM 115 的内部存储器 220 中而不是在存储单元 206 中，如图 3 所示。密码信息可被加密，尤其是如果储存在 TPM 115 外部的時候。

图 4 示出了包括用图 2 的 TPM 115 实现的计算机系统 300 的平台的一个实施例。计算机系统 300 包括总线 302 和耦合到总线 302 的处理器 310。计算机系统 300 还包括主存储器单元 304 和静态存储器单元 306。

此处，主存储器单元 304 是用于储存信息和由处理器 310 执行的指令的易失性半导体存储器。主存储器 304 还可用于在处理器 310 执行指令期间储存临时变量或其它中间信息。静态存储器单元 306 是用于更持久地为处理器 310 储存信息和指令的非易失性半导体存储器。静态存储器 306 的示例包括但不限于或不约束于只读存储器 (ROM)。主存储器单元 304 和静态存储器单元 306 都耦合到总线 302。

在本发明的一个实施例中，计算机系统 300 还包括诸如磁盘或光盘等数据存储设备 308，且其相应的驱动器也可耦合到计算机系统 300 用于储存信息和指令。

计算机系统 300 也可经由总线 302 耦合到图形控制器设备 314，该设备控制诸如阴极射线管 (CRT)、液晶显示器 (LCD) 或任何平板显示器等显示器，用于向最终用户显示信息。在一个实施例中，可以期望图形控制器或其它外围设备能够建立与由处理器执行的软件模块的经认证的加密通信会话。

通常，字母数字输入设备 316 (例如，键盘、键区等) 可以耦合到总线 302，

用于向处理器 310 传递信息和/或命令选择。另一种类型的用户输入设备是光标控制单元 318, 诸如鼠标、跟踪球、触摸垫、输入笔或光标方向键, 用于向处理器 310 传递方向信息和命令选择并用于控制光标在显示器 314 上的移动。

通信接口单元 320 也耦合到总线 302。接口单元 320 的示例包括调制解调器、网络接口卡或用于耦合到形成局域网或广域网一部分的通信链路的其它公知接口。以此方式, 计算机系统 300 可例如经由诸如公司的内联网和/或互联网耦合到多个客户机和/或服务器。

可以理解, 对某些实现而言可能需要比上述的更少或更多的装备的计算机系统。因此, 计算机系统 300 的配置取决于诸如价格约束、性能要求、技术改进和/或其它环境等众多因素而在各个实现之间不同。

在至少一个实施例中, 计算机系统 300 可支持使用存储在主存储器 304 和/或大容量存储设备 308 中并由处理器 310 执行的特别保护的“可信”软件模块(例如, 防篡改软件或具有运行受保护程序的能力的系统), 以在即使系统中存在其它恶意软件的情况下也执行特定活动。这些可信软件模块中的某一些需要不仅对其它平台, 而且对同一平台中的一个或多个设备, 诸如图形控制器 314 的同等“可信”的受保护访问。一般而言, 这一访问要求可信软件模块能够标识设备的能力和/或特定身份, 然后建立与该设备的加密会话以允许交换不能被系统中的其它软件监听或欺诈的数据。

标识设备同时建立加密会话的一种现有技术方法是使用单侧经认证的 Diffie-Helman (DH) 密钥交换过程。在该过程中, 向设备分配一唯一的公有/私有 RSA 或 ECC 密钥对。设备保持并保护私钥, 而公钥连同认证证书一起可被发放到软件模块。在 DH 密钥交换过程中, 设备使用其私钥来签署消息, 软件模块可使用相应的公钥来验证该私钥。这允许软件模块认证消息确实是来自感兴趣的设备。

然而, 由于这一认证过程使用 RSA 或 ECC 密钥, 因此设备具有唯一且可证明的身份。可使该设备用其私钥签署消息的任何软件模块能证明该特定的唯一设备存在于计算机系统中。假设设备很少在处理系统之间迁移, 则这也表示可证明的唯一计算机系统身份。此外, 设备的公钥本身表示恒定的唯一值; 这实际上是一个永久的“cookie”。在某些情况下, 这些特性可被解释为严重的私密性问题。

在 2004 年? 月? 日提交的名为 “An Apparatus and Method for Establishing an Authenticated Encrypted Session with a Device Without Exposeing Privacy-Sensitive Information” (用于在不揭露私密性敏感信息的情况下建立与设备的经认证的加密

会话的装置和方法)、转让给本申请的所有者的共同待批的专利申请第 10/???,??? 号中描述了一种替换方法。在该方法中,单侧经认证的 Diffie-Helman 过程中对 RSA 或 ECC 密钥的使用用直接证明密钥来替换。使用该方法的设备可被认证为属于一特定的设备族,这可包括关于该设备的行为或可信性的保证。该方法不揭露能用于建立表示处理系统的唯一身份的任何唯一标识信息。

尽管该方法能良好地起作用,但是它需要设备中的额外存储来保持直接证明私钥,该私钥可能大于 RSA 或 ECC 密钥。为减轻该额外存储要求的负担,本发明的实施例定义了一种用于在需要密钥时确保设备具有直接证明私钥而无需设备中的实际附加存储的系统和过程。在一个实施例中,按签署组向客户机计算机系统传递 DP 密钥。

在本发明的至少一个实施例中,在生产线上生产设备时,设备制造商仅将 128 位的伪随机数储存到该设备中,同时使用分发 CD 来加密并传递大得多的直接证明私钥(DPpri)。其它实施例可将长于或短于 128 位的数字储存到设备中。该过程确保只有指定的设备才能解密和使用其签署的 DPpri 密钥。

在本发明的至少一个实施例中,可以按由设备制造商签署的组记录来传递用 DPpri 加密的称为“密钥块(keyblob)”的数据结构。整个组记录必须被传递到设备,而设备仅提取其自己的加密的密钥块。通过要求设备对整个记录进行语法分析,并且仅在对整个记录进行语法分析之后才开始处理所提取的密钥块,攻击者就无法基于定时攻击来推断选择了哪一密钥块。通过签署该记录,并要求设备在处理其密钥块之前验证签名,可以确保攻击者无法提供单个密钥块的多个副本来测试设备的响应。在一个实施例中,攻击者最多能确定的也就是设备是组的一个成员。在一个实施例中,设备储存预定大小(例如,128 位)的伪随机值、组标识符(例如,4 字节)和 20 字节的设备制造商组公钥的散列,总共约 40 字节的数据。

图 5 是根据本发明的一个实施例用于按签署组来分发直接证明密钥的系统 500 的图示。该系统中有三个实体,即设备制造受保护系统 502、设备制造生产系统 503 以及客户机计算机系统 504。设备制造受保护系统包括在设备 506 的制造之前的设置过程中使用的处理系统。受保护系统 502 可由设备制造商或其它实体操作,以使受保护系统被保护不受来自设备制造方(例如,它在封闭系统中)之外的黑客的攻击。制造生产系统 503 可在设备的制造中使用。在一个实施例中,受保护系统和生产系统可以是同一系统。设备 506 包括用于包括在客户机计算机系统(例如,存储器控制器、诸如图形控制器等外围设备、I/O 设备、其它设备等)中的任

何硬件设备。在本发明的实施例中，设备包括储存在设备的非易失性存储中的伪随机值 RAND 508 和组序号 509。

制造受保护系统包括受保护数据库 510 和生成功能 512。受保护数据库包括用于储存由生成功能 512 用下述方式生成的多个伪随机值(至少是对每一要制造的设备有一个那样多)的数据结构。生成功能包括生成此处称为密钥块 514 的数据结构的逻辑(以软件或硬件实现)。密钥块 514 包括至少三个数据项。唯一直接证明私钥(DPpri)包括可由设备用于签署的密码密钥。DP 私有摘要 516(DPpri 摘要)包括根据诸如 SHA-1 等生成安全消息摘要的任何公知方法的 DPpri 的消息摘要。某些实施例可包括伪随机初始化向量(IV) 518，该向量包括因兼容性目的而作为密钥块的一部分的比特流。如果对加密使用流密码，则以用于在流密码中使用 IV 的公知方法来使用 IV。如果对加密使用块密码，则 IV 将用作要加密的消息的一部分，由此使得加密的每一实例都是不同的。

在本发明的实施例中，制造受保护系统生成一个或多个密钥块(如以下详细描述)，并将该密钥块按组记录 515 储存在 CD 522 上的密钥块数据库 520 中。在一个实施例中，按任何组合，，在单个 CD 上的每一组记录中可以有多多个密钥块和多个组记录，唯一的限制是 CD 的物理存储限制。由此，每一组记录包括多个密钥块。CD 然后通过典型的物理通道分发到计算机系统制造商、计算机销售商、客户机计算机系统消费者和其他人。尽管此处 CD 被描述为存储介质，但是可使用任何合适的可移动存储介质(例如，数字多功能盘(DVD)或其它介质)。

期望使用直接证明协议来进行与系统 504 中包括的设备 506 的通信会话的认证和密钥交换的客户机计算机系统 504 可在一旦 CD 被插入到客户机计算机系统的 CDROM 驱动器(未示出)中之后即从 CD 上的密钥块数据库 520 中读出所选择的组记录 515。密钥块数据可从组记录中获得，并由设备用于生成用于实现直接证明协议的本地化密钥块 524(如下所述)。在本发明的实施例中，包括多个密钥块的整个组记录由设备一次性地处理，并且攻击者可能无法确定实际使用哪个特定密钥块来生成加密的本地化密钥块。设备驱动程序软件 526 由客户机计算机系统执行来初始化并控制设备 506。

在本发明的实施例中，可以有四个不同的操作阶段。图 6 是示出根据本发明的一个实施例的分发直接证明密钥的方法的各阶段的流程图 600。根据本发明的实施例，可在每一阶段执行特定动作。在设备制造商方，至少有两个阶段：设置阶段 602 和制造产品阶段 604。设置阶段此处参考图 7 来描述。制造产品阶段此处参考

图 8 来描述。在具有客户机计算机系统的消费者方，有至少两个阶段：设置阶段 606 和使用阶段 608。客户机计算机系统设置阶段此处参考图 9 来描述。客户机计算机系统使用阶段此处参考图 10 来描述。

图 7 和 8 是示出根据本发明的一个实施例的设备制造设置处理的流程图 700 和 800。在一个实施例中，设备制造商可使用制造受保护系统 502 来执行这些动作。在框 701 处，设备制造商为要制造的每一设备类生成直接证明族密钥对（Fpub 和 Fpri）。每一唯一设备将具有相应的 DPpri 密钥，使得使用 DPpri 创建的签名可通过 Fpub 来验证。一个设备类可包括设备的任何集合或子集，诸如选中的产品线（即，设备类型）或基于版本号的产品线子集，或设备的其它特性。族密钥对由为其生成该密钥对的设备类使用。

在框 702 处，设备制造商生成将用于签署和验证组记录的 RSA 密钥对（Gpri，Gpub）。在其它实施例中，可使用任何安全数字签名系统来代替 RSA。该密钥对独立于框 701 中生成的族密钥对，并可用于由设备制造商生成的所有设备分组。在框 703 处，设备制造商选择一期望的组大小。组大小可以是族中将被分组在一起的设备的数目。组大小被选为足够大以允许个别设备“隐藏”在组内，同时不大到在设备的密钥块提取处理期间消耗过多的时间。在一个实施例中，组大小可被选为 5,000 个设备。在其它实施例中，可使用其它大小。

设备制造商然后可生成由组大小指定的数目的设备密钥。具有由组大小指定的数目的设备的每一组可按组序号来指定。对于要对给定组制造的每一设备，生成功能 512 或制造受保护系统 502 的其它模块可执行图 7 的框 704 到图 8 的框 802。首先，在框 704 处，生成功能生成唯一伪随机值（RAND）508。在一个实施例中，RAND 的长度是 128 位。在其它实施例中，可使用其它大小的值。在一个实施例中，可事先生成用于多个设备的伪随机值。在框 706 处，使用设备支持的单向函数  $f$ ，生成功能从唯一 RAND 值中生成对称加密密钥 SKEY（ $SKEY=f(RAND)$ ）。单向函数可以是适用于此目的的任何已知算法（例如，SHA-1、MGF1、数据加密标准（DES）、三重 DES 等）。在框 708 处，在一个实施例中，生成功能通过使用 SKEY 来加密“空条目”（例如，少量零字节），来生成将用于引用分发 CD 522 上的该设备的密钥块 514 的标识符（ID）标签（设备 ID=使用 SKEY 加密(0..0)）。在其它实施例中，可使用生成设备 ID 的其它方法或可通过 SKEY 来加密其它值。

接着，在框 710 处，生成功能生成与设备的族公钥（Fpub）相关的 DP 私有签署密钥 DPpri。在框 712 处，生成功能使用已知的方法（例如，使用 SHA-1 或另一

散列算法)对 DPpri 进行散列运算以产生 DPpri 摘要。在框 714 处,生成功能为设备构建密钥块数据结构。密钥块至少包括 DPpri 和 DPpri 摘要。在一个实施例中,密钥块还包括具有多个伪随机地生成的位的随机初始化向量(IV)。这些值可使用 SKEY 来加密以产生经加密的密钥块 514。在框 716 处,框 708 处生成的设备 ID 和框 714 处生成的经加密的密钥块 514 可被储存在要在分发 CD 522 上发布的密钥块数据库 520 中的记录中。在一个实施例中,密钥块数据库中的记录可由设备 ID 来指示。

处理在图 8 的框 801 处继续。在框 801 处,当前 RAND 值和设备所属的组的当前组序号可被储存在受保护数据库 510 中。在框 802 处,可删除 SKEY 和 Dppri,因为它们将由设备现场重新生成。对将要制造的每一连续的设备组将组序号递增一。DPpri 摘要的创建和后续的通过 SKEY 的加密被设计成使得 DPpri 的内容不能被没有 SKEY 的任何实体确定,且使得密钥块的内容没有在随后被拥有 SKEY 的实体删除的情况下不能被没有 SKEY 的实体修改。在其它实施例中,可使用提供这一秘密和完整性保护的其它方法。在某些实施例中,可能不需要完整性保护,并且可使用仅提供秘密的方法。在这一情况下,DPpri 摘要的值可能不是必需的。

当为一组设备创建了密钥块的整个数据集时,至少签署该组的密钥块数据库 520 并将其刻录到常见的分发 CD 上,以随每一设备分发(在一个实施例中,当由设备 ID 字段所索引时,对每一设备可使用一个密钥块数据库条目)。由此,在框 804 处,设备制造商创建组记录 515。组记录包括组序号、组的公钥 Gpub、组大小以及整个组的密钥块记录(<组序号, Gpub, 组大小, <设备 ID1, 经加密的密钥块 1>, <设备 ID2, 经加密的密钥块 2>, ...>)。在框 806 处,设备制造商使用组私钥 Gpri 签署组记录,并将数字签名追加到该组记录。在框 808 处,可将经签署的组记录添加到分发 CD 上的密钥块数据库。在一个实施例中,分发 CD 还包括用于在客户机计算机系统上进行将来的处理的密钥检索实用程序软件模块,其使用在下文中更详细描述。

在框 802 之后的任何时刻,在框 810 处,可将 RAND 和组序号值对的受保护数据库安全地上传到制造商生产系统 503,该系统在制造过程期间将 RAND 和组序号值储存到设备中。一旦验证了这一上传,可从制造受保护系统 502 中安全地删除 RAND 值。

图 9 是示出根据本发明的一个实施例的设备制造生产处理的流程图 900。当在生产线上制造设备时,在框 902 处,制造生产系统从受保护数据库中选择一未使用

的 RAND 和组序号值对。所选择的 RAND 和组序号值然后可被储存在设备中的非易失性存储中。在一个实施例中，非易失性存储包括 TPM。在框 904 处，也可将组公钥 Gpub 的散列储存在设备的非易失性存储中。在框 906 处，一旦将 RAND 值成功储存到设备中，则制造生产系统毁去受保护数据库中该设备的 RAND 值的任何记录。此时，RAND 值的唯一副本储存在设备中。

在一个替换实施例中，RAND 值可在设备的制造期间创建，然后被发送到制造受保护系统以计算密钥块。

在另一实施例中，RAND 值可在设备上创建，并且设备和制造受保护系统可参与一协议以使用不在设备之外揭示 DPpri 密钥的方法来生成 DPpri 密钥。然后，设备可创建设备 ID、SKEY 和密钥块。设备将设备 ID 和密钥块传递到制造系统以储存在受保护数据库 510 中。在此方法中，制造系统最终在受保护数据库中有相同的信息（设备 ID，密钥块）而结束，但是不知道 RAND 或 DPpri 的值。

图 10 和 11 是根据本发明的一个实施例的客户机计算机系统设置处理的流程图 1000 和 1100。客户机计算机系统可执行这些动作作为引导系统的一部分。在框 1002 处，可以正常方式引导客户机计算机系统，并且可将设备的设备驱动程序 526 加载到主存储器中。当初始化了设备驱动程序并开始执行时，设备驱动程序在框 1004 处确定设备 506 的大容量存储设备 308 中是否已经储存了经加密的本地化密钥块 524。如果有，则无需执行进一步的设置处理，并且设置处理在框 1006 处结束。如果没有，则处理在框 1008 处继续。在框 1008 处，设备驱动程序使得向客户机计算机系统的用户显示请求插入分发 CD 522 的消息。一旦由计算机系统读取了 CD，设备驱动程序然后启动 CD 上储存的密钥检索实用程序软件模块（图 5 中未示出）。密钥检索实用程序向设备请求其组 ID，该组 ID 可以是组公钥 Gpub 和组序号 509 的散列。设备返回这些值，实用程序使用这些值来从 CD 上的密钥块数据库中定位正确的经签署的组记录。该实用程序还向设备 506 发出获取密钥命令以启动设备的 DP 私钥获取过程。

作为响应，在框 1010 处，设备使用其单向函数  $f$  来从嵌入的 RAND 值 508 中重新生成对称密钥 SKEY（现在用于解密）（ $SKEY=f(RAND)$ ）。在框 1012 处，设备然后通过使用 SKEY 加密“空条目”（例如，少量零值），来生成其唯一设备 ID 标签（设备 ID=使用 SKEY 加密(0..0)）。在本发明的一个实施例中，这些值没有一个在设备外部揭露。设备然后发信号通知其准备就绪以继续。

在框 1014 处，密钥检索实用程序在 CD 上的密钥块数据库 520 中搜索包含匹



配的组序号的组记录，提取组记录，并将整个组记录传输到设备。

在框 1016 处，设备对提供的整个组记录进行语法分析，但是仅保持组序号、组记录的散列、组公钥 Gpub 和匹配设备自己的设备 ID（在框 1012 中生成）的第一个<设备 ID，经加密的密钥块>字段。在框 1018 处，设备现在验证组记录。在一个实施例中，设备将所提取的组序号字段与嵌入在设备中的组序号进行比较。如果它们不匹配，则可终止密钥获取过程。如果匹配，则设备对所提取的 Gpub 字段进行散列运算，并将其与嵌入在设备中的 Gpub 散列进行比较。如果散列不匹配，则可终止密钥获取过程。如果匹配，则设备使用经确认的 Gpub 密钥来验证组记录的散列上所提供的签名。如果签名得到验证，则验证组记录，并且该过程在图 11 的框 1120 处继续。

在一个实施例中，如果欺诈软件试图在设备已有了密钥块之后向设备发送获取密钥命令，则设备不用组序号来响应该欺诈软件。相反，设备将返回一出错指示符。实际上，如果设备能够访问本地化密钥块，则获取密钥命令的功能被禁用。以此方式，设备除非在它没有密钥块的时候，否则不会揭示组序号。

在框 1120 处，设备使用对称密钥 SKEY 来解密经加密的密钥块，以产生 DPpri 和 DPpri 摘要，并将这些值储存在其非易失性存储（经解密的密钥块=使用 SKEY 解密(IV, DPpri, DPpri 摘要)）。可丢弃初始化向量（IV）。在框 1122 处，设备然后通过 DPpri 进行散列运算并将结果与 DPpri 摘要进行比较来核查 DPpri 的完整性。如果比较良好，则设备接受 DPpri 作为其有效密钥。设备也可将密钥已获取标志设为真来指示 DP 私钥已被成功获取。在框 1124 处，设备选择一新的 IV，并使用该新的 IV 创建新的经加密的本地化密钥块（本地化密钥块=使用 SKEY 加密(IV2, DPpri, DPpri 摘要)）。新的经加密的本地化密钥块可被返回给密钥检索实用程序。在框 1126 处，密钥检索实用程序将该经加密的本地化密钥块储存在客户机计算机系统内的存储中（例如，诸如大容量存储设备 308）。设备的 DPpri 现在被安全地储存在客户机计算机系统中。

一旦设备在设置处理期间获取了 DPpri，设备然后可使用该 DPpri。图 12 是根据本发明的一个实施例的客户机计算机系统处理的流程图。客户机计算机系统可在完成设置之后的任何时刻执行这些动作。在框 1202 处，可以正常方式引导客户机计算机系统，并且可将设备的设备驱动程序 526 加载到主存储器中。当初始化了设备驱动程序并开始执行时，设备驱动程序确定设备 506 的大容量存储设备 308 中是否已储存了经加密的本地化密钥块 524。如果没有，则执行图 10 和 11 的设置处理。

如果对该设备有经加密的本地化密钥块可用，则处理在框 1206 处继续。在框 1206 处，设备驱动程序检索经加密的本地化密钥块，并将该密钥块传递到设备。在一个实施例中，密钥块的传递可通过执行加载密钥块命令来完成。

在框 1208 处，设备使用其单向函数  $f$  来从嵌入的 RAND 值 508 重新生成对称密钥 SKEY（现在用于解密）（ $SKEY=f(RAND)$ ）。在框 1210 处，设备使用对称密钥 SKEY 解密经加密的本地化密钥块，以产生 DPpri 和 DPpri 摘要，并将这些值储存在其非易失性存储中（经解密的密钥块=使用 SKEY 解密(IV2, DPpri, DPpri 摘要)）。可丢弃第二初始化向量 (IV2)。在框 1212 处，设备通过对 DPpri 进行散列运算并将结果与 DPpri 摘要进行比较来核查 DPpri 的完整性。如果比较良好（例如，摘要匹配），则设备接收该 DPpri 作为先前获取的有效密钥，并允许使用它。设备也可将密钥已获取标志设为真来指示已成功获取 DP 私钥。在框 1214 处，设备选择另外一个 IV，并使用该新的 IV 来创建新的经加密的本地化密钥块（本地化密钥块=使用 SKEY 加密(IV3, DPpri, DPpri 摘要)）。该新的经加密的本地化密钥块可被返回给密钥检索实用程序。在框 1216 处，密钥检索实用程序将该经加密的本地化密钥块储存在客户机计算机系统的存储中（例如，诸如大容量存储设备 308）。设备的 DPpri 现在被再一次安全地储存在客户机计算机系统中。

在本发明的一个实施例中，不必一次为经签署的组生成所有设备 DP 私钥。假定分发 CD 是定期更新的，则设备 DP 私钥可在需要时批量生成。每次“刻录”分发 CD 时，它将包含迄今生成的密钥块数据库的经签署的组，包括已生成但是尚未分配给设备的那些设备密钥。

在一个实施例中，当如图 10 的框 1018 中那样处理整个组记录时，如果设备检测到错误，则设备可设置指示发生了错误的标志，但是应继续处理。当对系统设置完成了所有的步骤时，设备然后可向设备驱动程序发信号通知该错误。这可阻止攻击者从错误类型和位置中获取信息。

在一个实施例中，此处所描述的方法可使用设备中的非易失性存储的大约 40 字节。在另一实施例中，如果在设备的经加密的密钥块中包括 Gpub 密钥散列而非将其储存在设备上的非易失性存储中，则这可减少到大约 20 字节。在这一情况下，当设备解密该经加密的密钥块时，设备可检索 Gpub 散列，使用该散列来核查 Gpub 密钥，并使用 Gpub 密钥来核查整个组记录上的签名。

尽管此处所讨论的操作可被描述为顺序的过程，但是某些操作实际上可以并行或同时执行。另外，在某些实施例中，可重新排列操作的次序而不脱离本发明的

精神。

此处所描述的教导不限于任何特定的硬件或软件配置；它们可适用于任何计算或处理环境。这些技术可用硬件、软件或两者的组合来实现。这些技术可用在诸如移动或固定计算机、个人数字助理、机顶盒、蜂窝电话和寻呼机、以及其它电子设备等可编程机器上执行的程序来实现，这些可编程机器均包括处理器、可由处理器读取的存储介质（包括易失性和非易失性存储器和/或存储元件）、至少一个输入设备以及一个或多个输出设备。向使用输入设备输入的数据应用程序代码以执行所描述的功能并生成输出信息。输出信息可被应用于一个或多个输出设备。本领域的普通技术人员可以理解，本发明可用各种计算机系统配置来实施，包括多处理器系统、小型机、大型计算机等。本发明也可在分布式计算环境中实现，在分布式计算环境中，任务可由通过通信网络链接的远程处理设备来执行。

每一程序可以用高级过程语言或面向对象的编程语言来实现以与处理系统通信。然而，如有所需，程序可用汇编语言或机器语言来实现。在任何情况下，语言都可以是已编译或已解释的。

程序指令可用于使得用该指令编程的通用或专用处理系统执行此处所描述的操作。或者，操作可由包含用于执行操作的硬连线逻辑的特定硬件组件或由已编程计算机组件和自定义硬件组件的任何组合来实现。此处所描述的方法可作为计算机程序产品来提供，计算机程序产品可包括其上储存有可用于对处理系统或其它电子设备编程以执行方法的指令的机器可读介质。此处使用的术语“机器可读介质”应包括能够储存或编码指令序列以供机器执行并使机器执行此处所描述的方法的任一种的任何介质。术语“机器可读介质”相应地应包括但不限于，固态存储器、光盘和磁盘、以及编码数据信号的载波。此外，本领域中通常以一种或另一种形式（例如，程序、过程、进程、应用程序、模块、逻辑等）将软件说成是采取动作或导致结果。这一表达仅仅是陈述处理系统对软件的执行使处理器执行产生结果的动作的简化方式。

尽管本发明是参考说明性实施例来描述的，但是该描述并不旨在以限制的意义来解释。对本发明所属领域的技术人员显而易见的对说明性实施例以及本发明的其它实施例的各种修改被认为落入本发明的精神和范围之内。

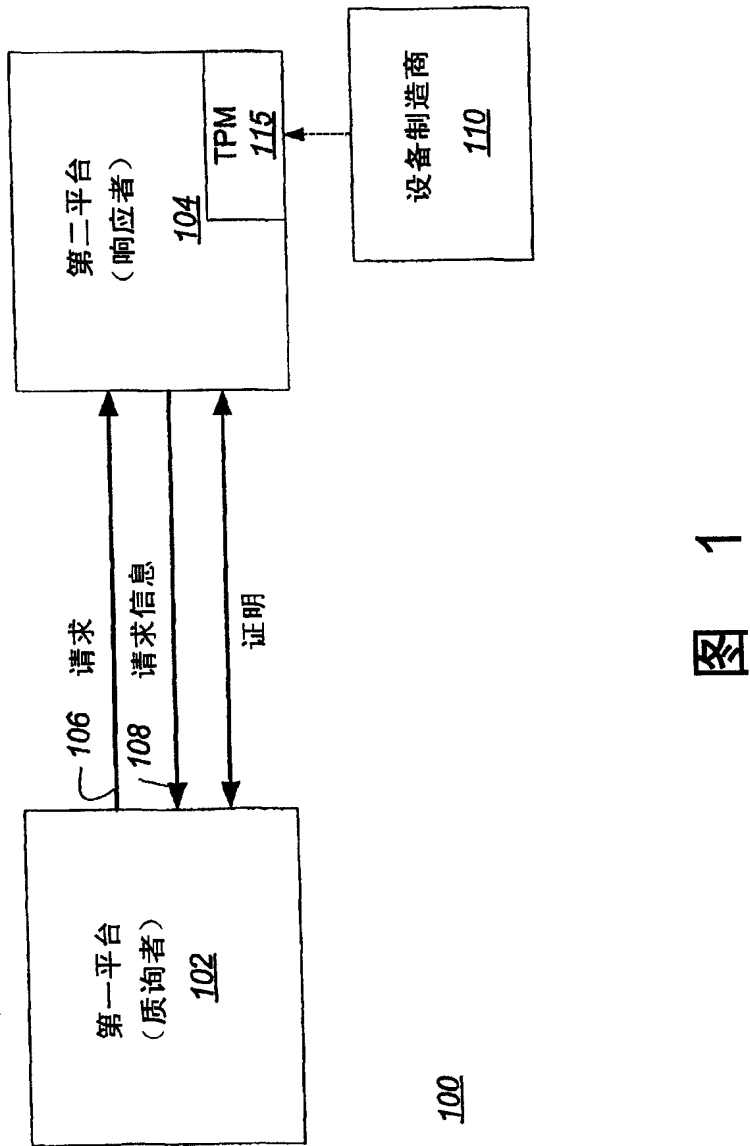


图 1

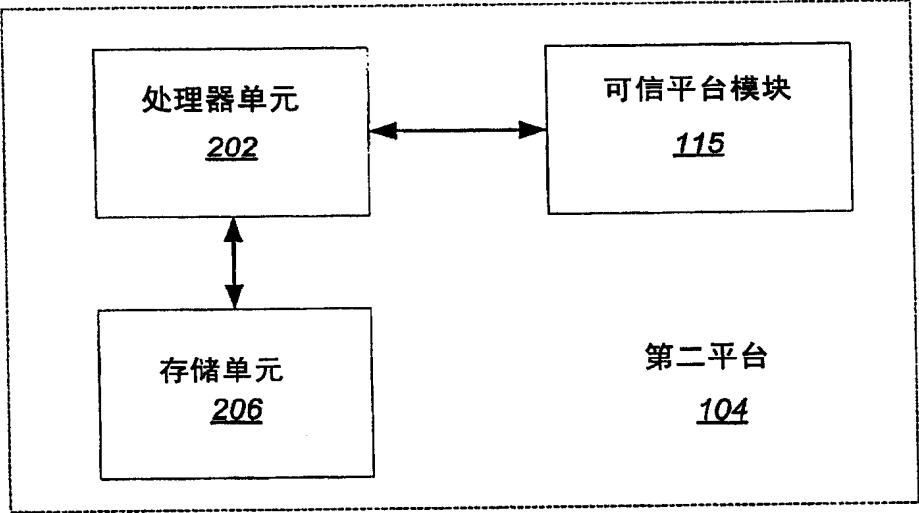


图 2

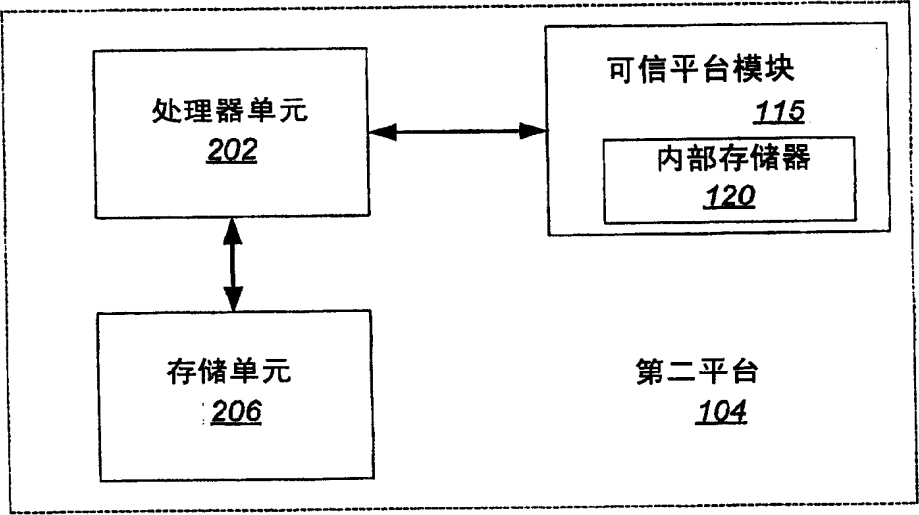
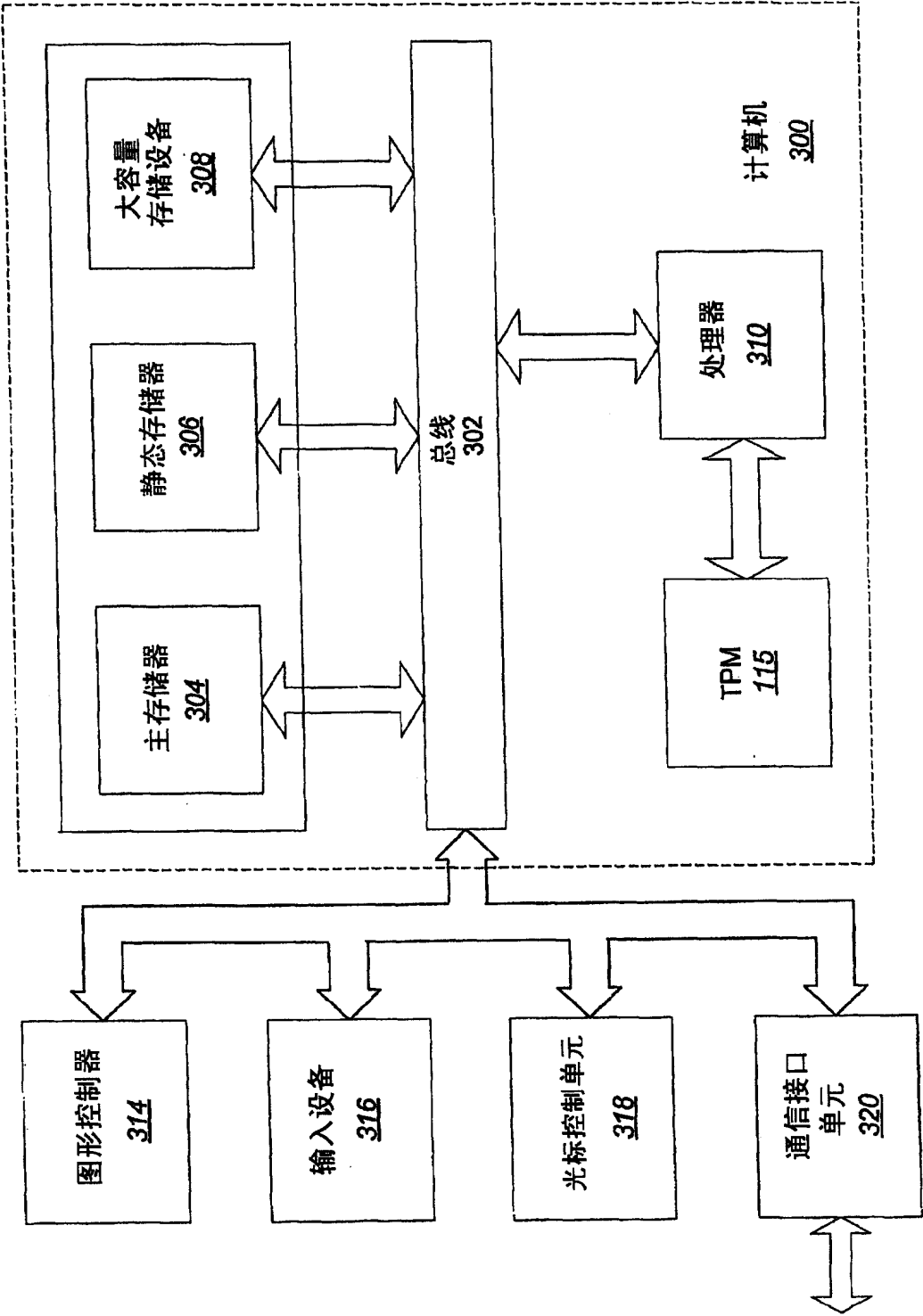


图 3



104

图 4

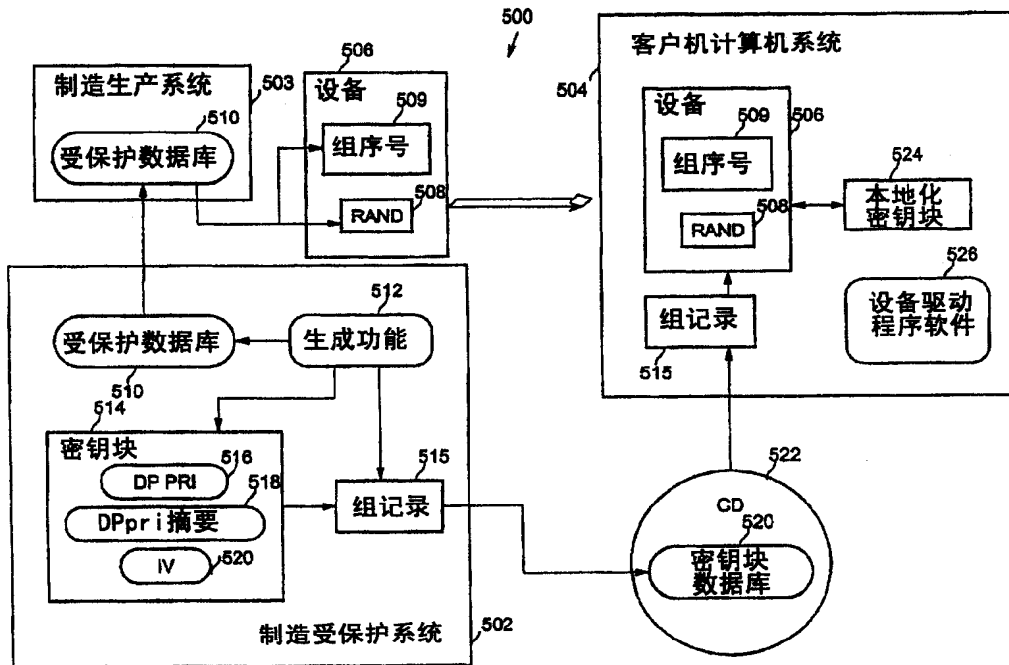


图 5

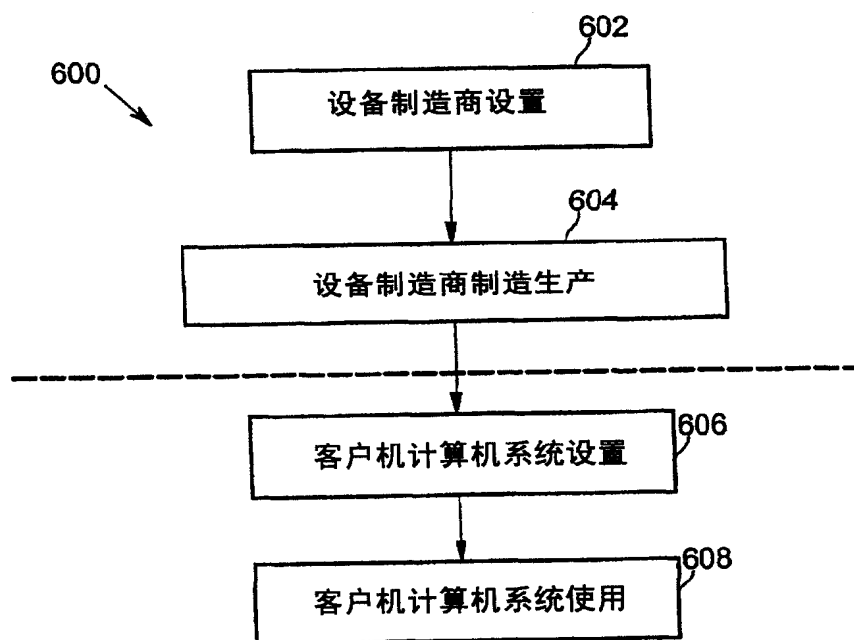


图 6



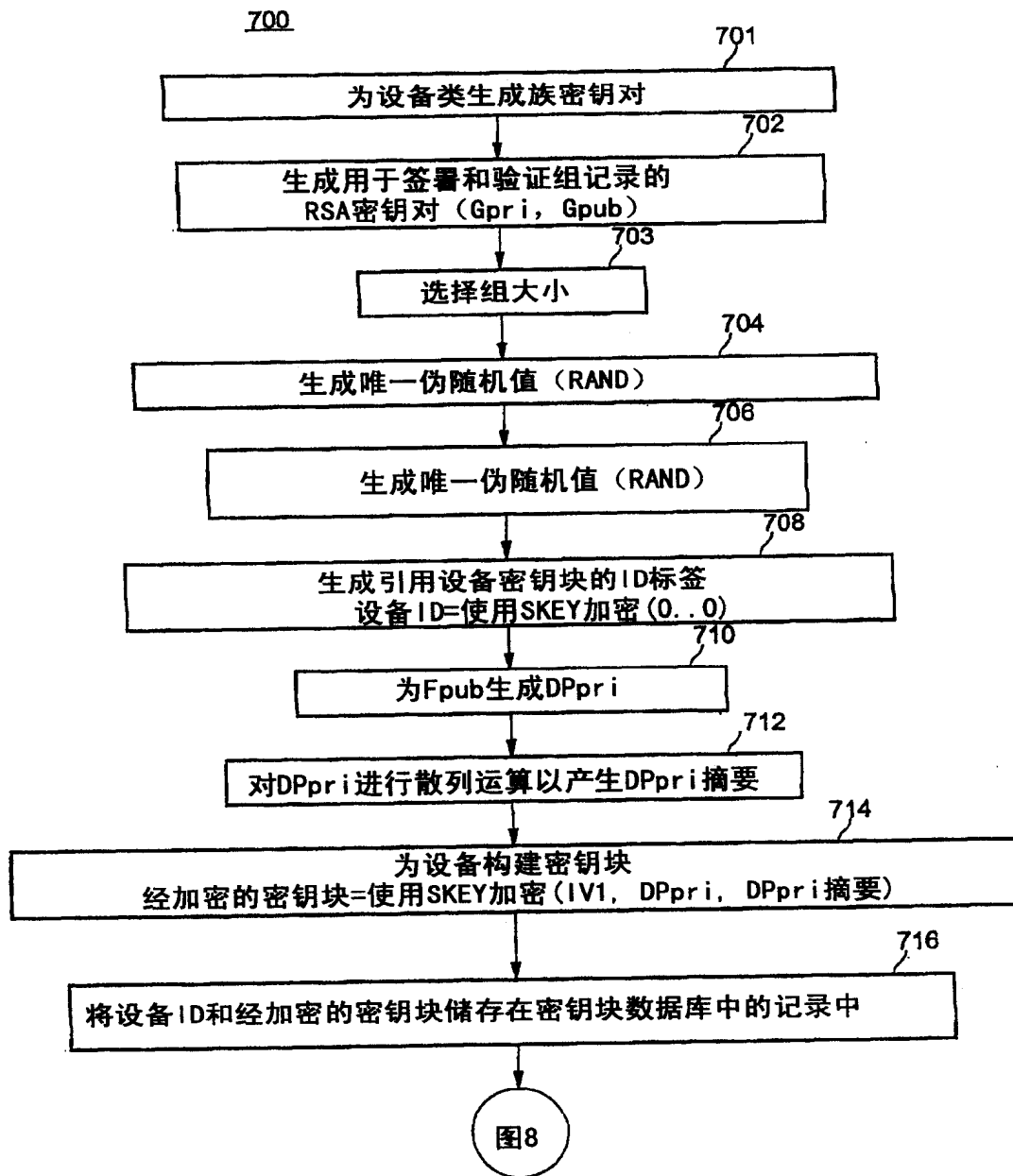


图 7

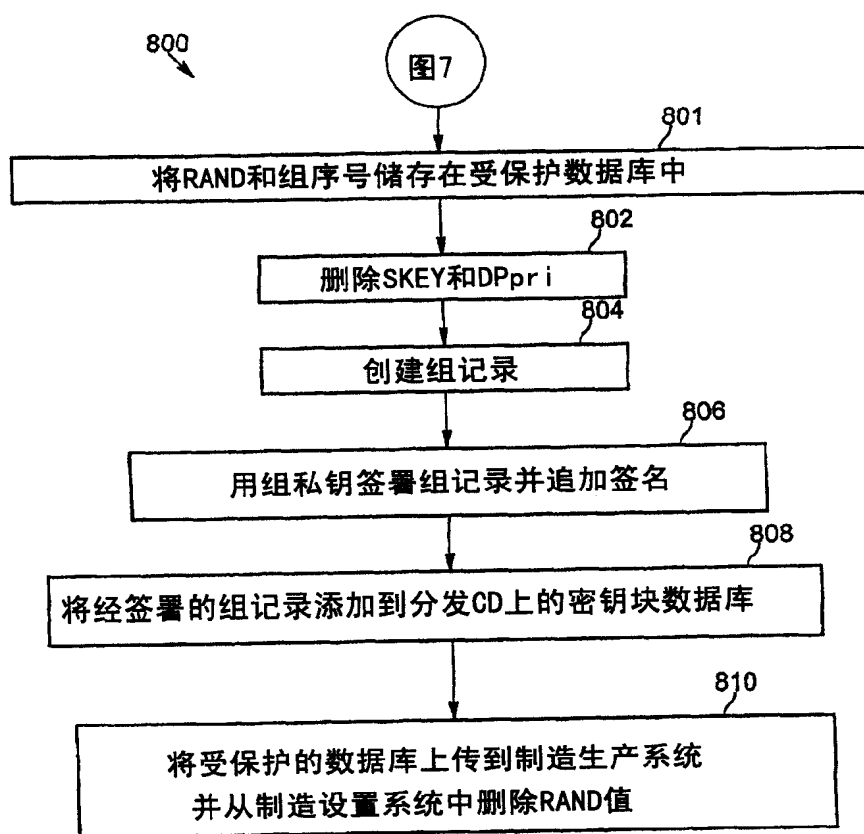


图 8

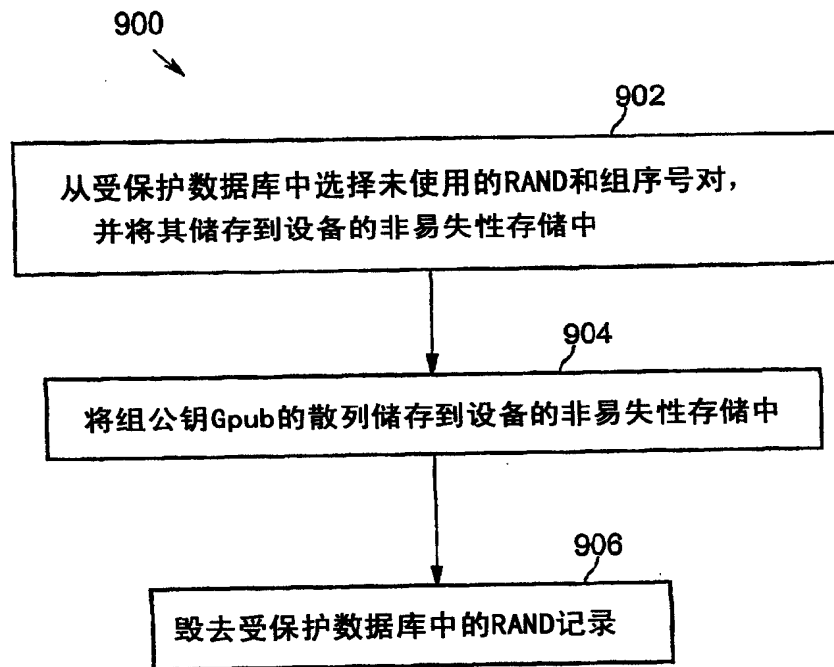


图 9

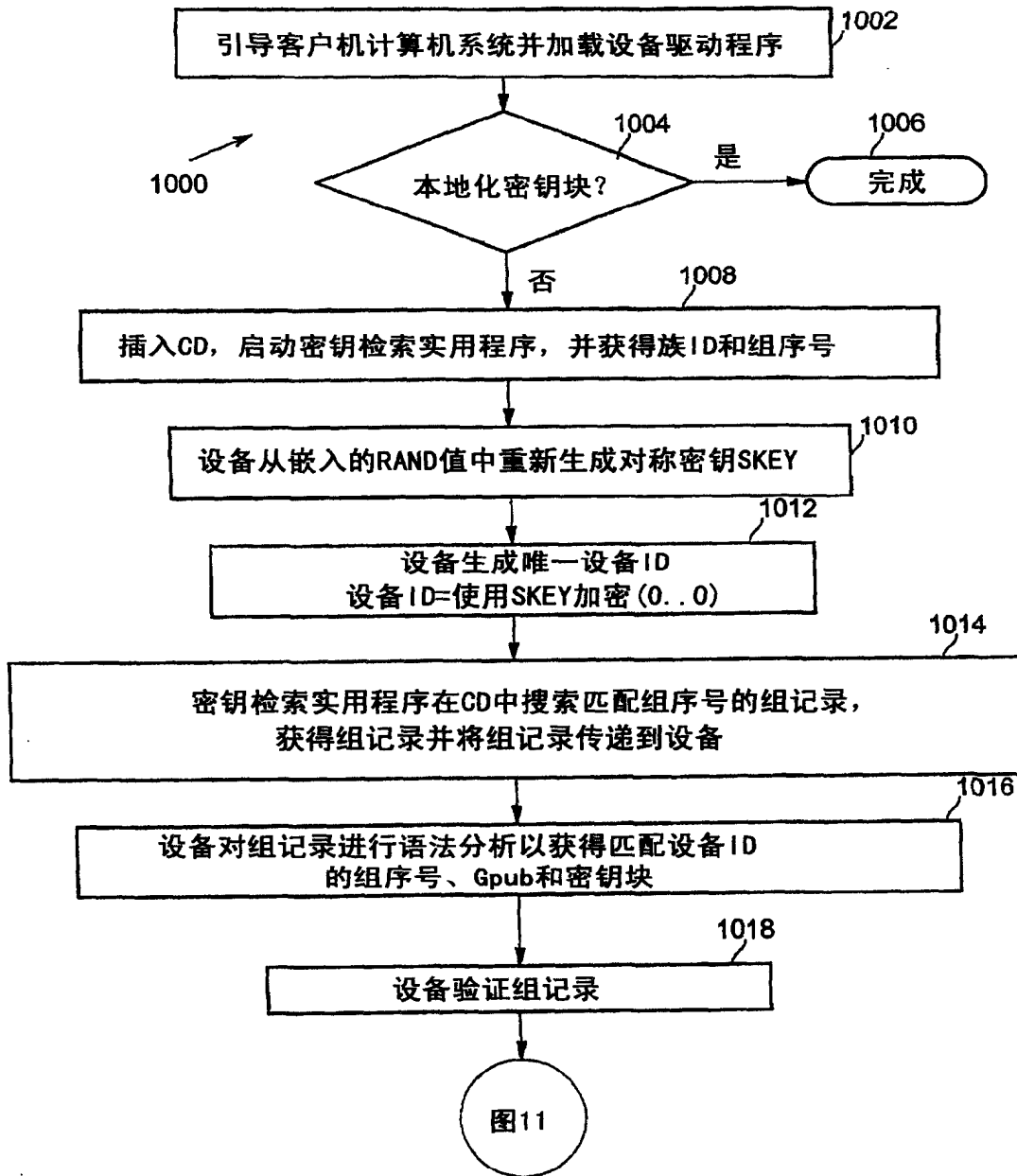


图 10

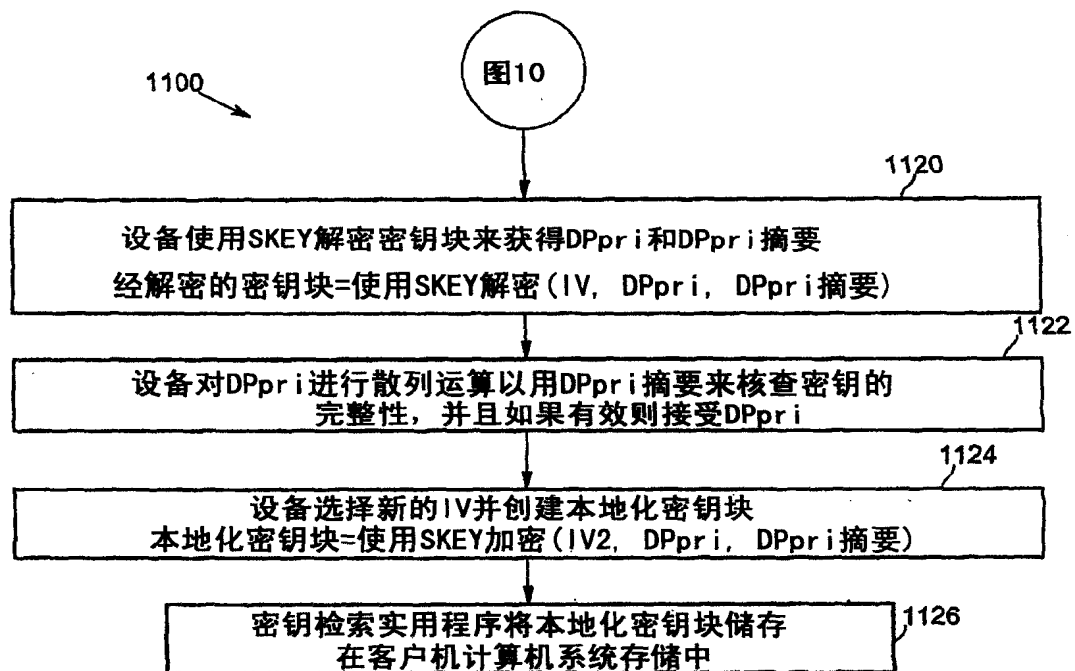


图 11

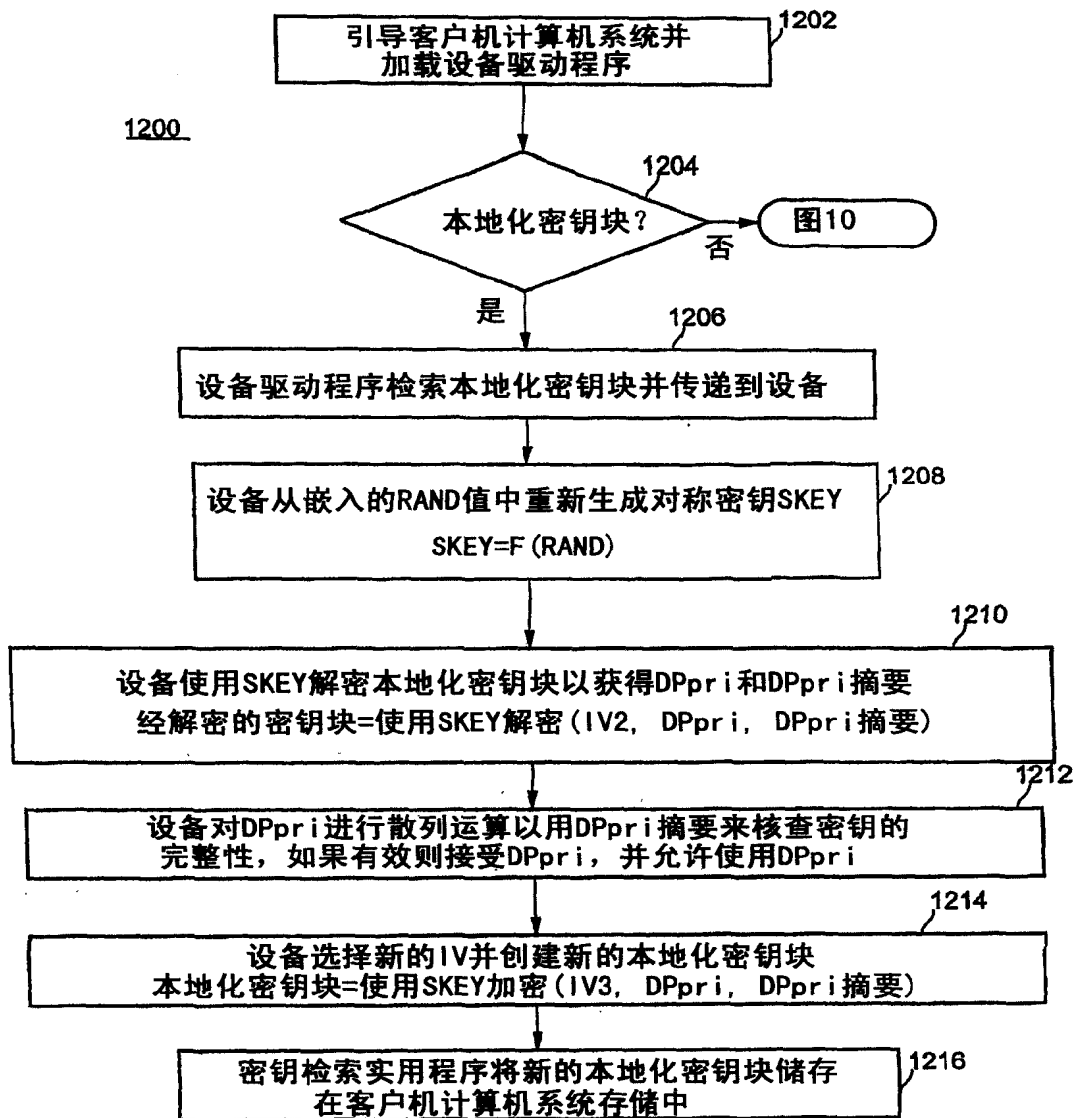


图 12